IOT ANALYTICS

QUECTEL

Securing the Cellular IoT Ecosystem: Trends, Regulations, and Supply Chain Best Practices

The world is getting ever more connected, but it needs to be secured

By the end of 2023, there were 16.6 billion connected IoT devices, reflecting 15% growth over 2022. IoT Analytics expects this number to grow by 13%, reaching 18.8 billion by the end of 2024. Additionally, global cellular IoT connections reached 3.6 billion in 2023, representing 21% of all global IoT connections. These connections are projected to grow at a 15% CAGR between 2024 and 2030.

As more devices become interconnected, more data is being shared. Many devices are even becoming more intelligent, with the ability to analyze and implement actions. These two facts bring about the need for greater device security to protect against malicious attacks. Robust hardware and software at the device level, within networks, and on cloud servers are ideal IoT security solutions.

IoT module security at the center of attention

IoT device security has been at the center of attention across Europe and the US the last year. The Cyber Trust Mark in the U.S is a new cybersecurity labeling initiative launched by the Federal Communications Commission (FCC) to help consumers easily identify smart devices that meet certain cybersecurity standards. Announced in 2023, this voluntary labeling program is designed for devices like smart home cameras, routers, thermostats, and other Internet of Things (IoT) products.

In Europe, the Council of the European Union adopted the EU CRA on October 10, 2024. The Act is set to enter into force in the second half of 2024, with IoT manufacturers required to place compliant products on the EU market by 2027. These are examples that IoT cyber security requirements are evolving quickly across the global scene.

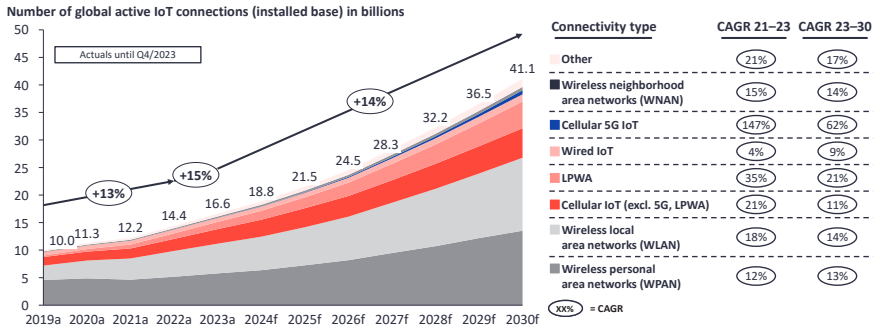
According to IoT Analytics' Global Cellular IoT Module and Chipset Market Tracker & Forecast Q2 2024, approximately 29% of cellular IoT modules shipped in Q2 2024 had no dedicated protection features. Only 33% had hardware-based security, and 38% had non-hardware-based security that relies on embedded software mechanisms or integrated features within existing hardware to create a secure environment.

Next, we spotlight cellular IoT module security by examining key cybersecurity regulations and their impact on IoT module supply chain security—both for the hardware, firmware and software used.

By the end of 2023, there were 16.6 billion connected IoT devices

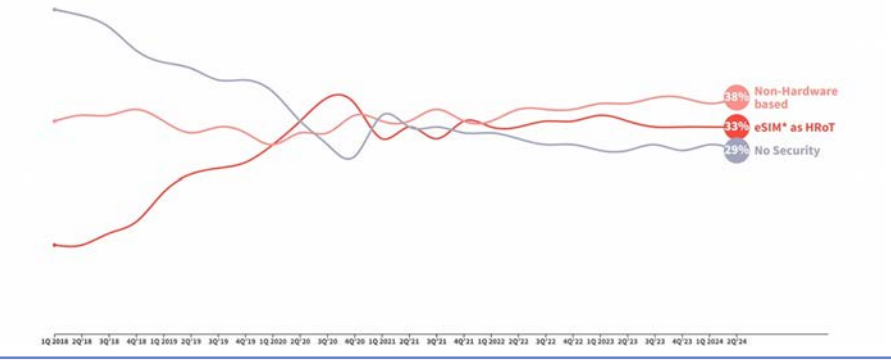
Global IoT market forecast: The world is getting ever more connected

Cellular IoT Connections reached 3.5 Billion of IoT Connection in 2023



Cellular IoT modules 2018-2024: The rise of hardware security

Cellular IoT module market share by security type (based on shipments in %)



Security considerations for software in the IoT module supply chain

Software vulnerabilities can result in wide-scale cyberattacks, making software supply chain security a top priority for businesses and regulators. Indeed, as cellular IoT modules become integral to critical infrastructure, national and regional governments have started passing or issuing strict cybersecurity regulations.

A selection of approaches to software supply chain vulnerabilities and related regulations are shared below.

Software bill of materials

A software bill of materials (SBOM) is a formal record containing detailed information about the components and supply chain relationships involved in software creation. For example, manufacturers use SBOMs to verify that no vulnerable or unauthorized software components are introduced during firmware updates, ensuring ongoing device security. SBOMs enhance the security of IoT products and cellular IoT modules by providing detailed visibility into software components, allowing manufacturers to identify and address vulnerabilities efficiently.

Aiding SBOMs are vulnerability exploitability exchange (VEX) documents. These structured documents provide additional context about the exploitability of known vulnerabilities listed in an SBOM. While an SBOM identifies software components and associated vulnerabilities, VEX documents specify whether these vulnerabilities are exploitable in a particular environment or have been mitigated. They help organizations prioritize their response to potential security risks and manage vulnerabilities more effectively throughout the software lifecycle.

Manufacturers use SBOMs to verify that no vulnerable or unauthorized software components are introduced during firmware updates, ensuring ongoing device security

Notable regulations related to SBOMs

- **US Executive Order (EO) 14028** – This US presidential order mandates that federal software suppliers in the US comply with the minimum elements of an SBOM set by the US Department of Commerce. Non-compliance potentially leads to disqualification from government contracts. Additionally, while this order does not explicitly mandate VEX documents, these documents are anticipated to become a de facto standard for enhancing software supply chain security, as it allows federal software suppliers to manage risks effectively and comply with various cybersecurity requirements.
- **EU Cyber Resilience Act (CRA)** – Unlike the U.S. regulation, the CRA applies to all vendors producing products with digital components connected to the Internet within the EU. The CRA makes SBOMs mandatory but does not require them to be made public, but they must be shared with national designated authorities. Like US EO 14028, the CRA does not specifically mention VEX. However, it promotes transparency and effective vulnerability management, which align with the objective of VEX documents.

Cryptographic signatures/hashes to tie reports to artifacts

Cryptographic signatures and hashes are essential for ensuring the integrity of software components within IoT devices. They help verify that software updates and components have not been tampered with during distribution or implementation. For cellular IoT devices, cryptographic signatures are particularly crucial for verifying software updates and firmware integrity, ensuring a secure boot process, and preventing unauthorized code from being executed.

Though regulations do not specifically direct the use of cryptographic signatures and hashes, US NIST SP 800-213 promotes organizational awareness of cryptographic security (namely, the Cryptographic Module Validation Program). Further, the EU CRA emphasizes the need to protect data integrity when being transmitted or stored, which this approach can assist with.

Country of origin

The country of origin of software components has become increasingly important as part of supply chain security. By understanding where software derives from will help mitigate risks by ensuring software components in cellular IoT modules can be identified and tracked to origin and ensure it comes with robust cybersecurity practices, reducing the likelihood of incorporating compromised or insecure elements into IoT devices.

Notable regulations related to country of origin

- **US Department of Defense Trusted Foundry Program and EO 13873** – These actions by the US government focus on identifying and mitigating risks associated with software and hardware originating from regions with less-than-rigorous cybersecurity standards
- **EU CRA** – Along with the aforementioned actions, this act also encourages transparency regarding a software's country of origin.

The country of origin of software components has become increasingly important as part of supply chain security

Security considerations for hardware in the IoT module supply chain

Software and network security solutions have historically overshadowed hardware security in IoT due to their visibility and simpler implementation, while hardware security is often more complex and costly. However, hardware-based security allows manufacturers and consumers to ensure module authenticity, addressing cloning, counterfeiting, and key protection. Once the security of keys is guaranteed, additional components like TrustZone and secure boot can be added. For IoT, eSIM and iSIM are hardware-based security elements, supported by initiatives like IoT SAFE.

A selection of approaches to hardware supply chain vulnerabilities and related regulations are shared below.

Penetration testing

A penetration test—often referred to as a pen test—is an authorized attempt by security experts ("red team") to carry out a cyberattack on a computer or network to test for exploitations. Pen testing is particularly important for IoT modules that serve critical infrastructure sectors, as these tests help identify weaknesses that malicious actors could exploit.

Notable regulations related to penetration tests

- **US EO 14028** – This EO promotes the establishment of minimum standards for vendors' testing of their software source code, including recommending types of manual and automated testing, such as pen testing.
- **EU CRA** – Among the many other guidelines listed above, this Act requires manufacturers to perform regular risk assessments, including penetration testing, to identify and mitigate vulnerabilities in their hardware and software products.

Origin of underlying hardware/technology (trusted vendors)

Scrutiny of the country of origin for software components helps ensure IoT modules adhere to the highest cybersecurity standards, protecting critical infrastructure from potential vulnerabilities.

Notable regulations related to the origin of underlying hardware/technology

- **US National Defense Authorization Act (NDAA) Section 889** – This section restricts federal procurement of telecommunications equipment from specific vendors deemed untrustworthy, emphasizing the importance of sourcing components from reliable manufacturers.
- **EU CRA** – The act calls for transparency in the sourcing and supply chain of hardware, ensuring that products entering the European market come from trusted vendors and comply with cybersecurity standards.

Hardware-based root of trust

A hardware-based root of trust (RoT) is a foundational security mechanism embedded directly in a device's hardware (e.g., the module). RoTs provide a trusted starting point for secure operations and ensure critical security functions—such as verifying the integrity of firmware, cryptographic key management, and secure boot processes—are protected from tampering and unauthorized access.

Notable regulations related to RoTs

Though regulations do not specifically direct the use of RoTs, they can be used with the origin of underlying hardware/technology approach to help validate the origins of components to meet regulations, such as the following:

- **US EO 13873** – This EO aims to prevent importing key information and communications technology from designated foreign adversaries, highlighting the importance of identifying and securing technology from trustworthy sources.
- **EU CRA** – The act advocates for hardware security measures—including RoT—and stresses transparency in the country of origin for hardware components to prevent the use of insecure elements from regions with lax cybersecurity standards.

Module vendor best practices for addressing cybersecurity regulation requirements

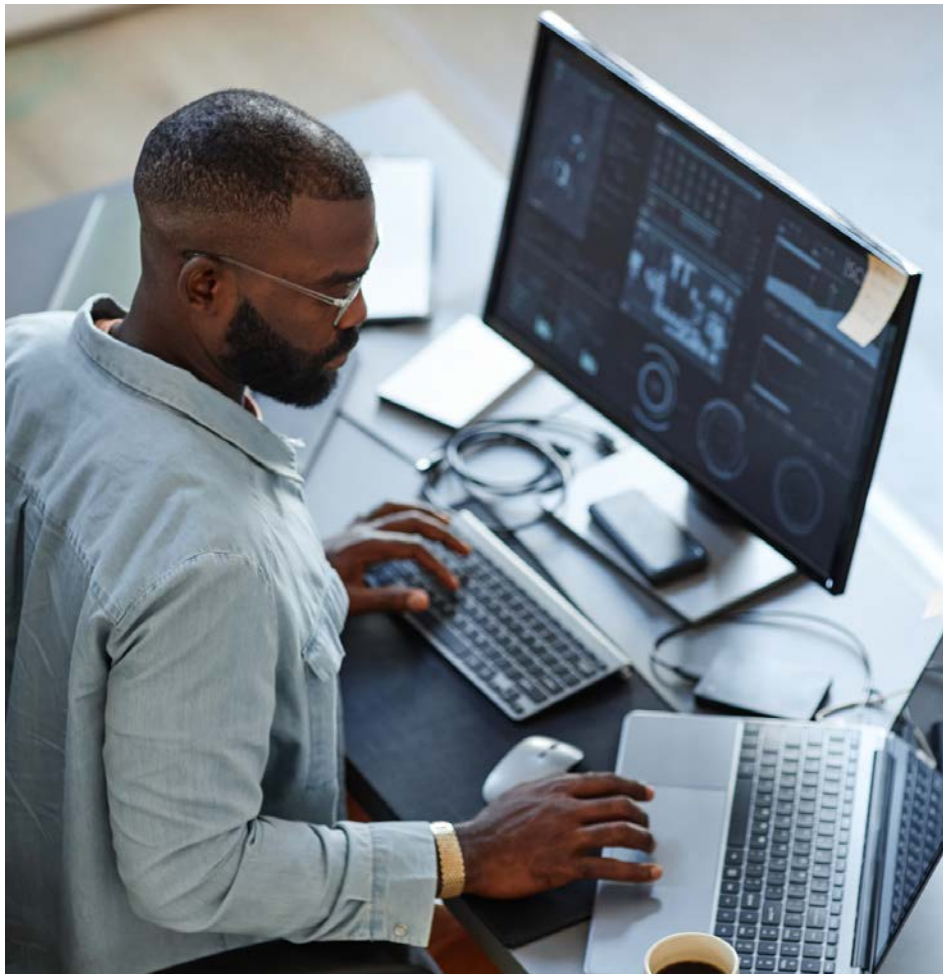
As cybersecurity regulations become increasingly stringent worldwide, cellular IoT module manufacturers are looking to implement practices to comply with these requirements. Below are some key strategies that IoT module vendors should employ to address software and hardware supply chain security regulations.

Software approach

On the software front, the vendors should take a multipronged approach. First, robust SBOM practices should be employed to prioritize transparency and traceability in software components. For example, an independent third-party company could conduct source and binary analysis to identify all software components, including open-source libraries. Vendors can then provide updated SBOM reports to customers and OEMs through secure web portals or other online mediums. Further, using tools like Coverity, Black Duck, and Finite State can help vendors cross-reference SBOM components with multiple vulnerability databases (e.g., NIST's National Vulnerability Database, the Common Weakness Enumeration system, and the Common Vulnerabilities and Exposures system) for prompt identification and mitigation of vulnerabilities. Vendors should also implement cryptographic techniques by computing secure hash algorithms and cryptographically signing them using a RoT certificate chain. Additionally, utilizing one-time programmable fuses in the system-on-chip (SoC) for boot verification aligns with US NIST and EU CRA standards.

"We have integrated more than one scanning tool into our DevSecOps, which will help our R&D team upload new firmware to the SCA platform and then generate SBOMs automatically."

Key leading vendor quote about SBOMs



Hardware approach

On the hardware front, vendors should incorporate several security practices to ensure security. For example, they can establish a foundational layer of protection by using standard public key infrastructure (commonly referred to as PKI) technology and store using the aforementioned cryptographic techniques. The SoC can feature a trust zone or trusted execution environment, supporting cryptographic functions and secure key storage. Additionally, vendors should ensure that hardware components originate from trusted sources to comply with U.S. EO 13873 and the EU CRA. Auditing and verifying the hardware supply chain, with SoC vendors providing necessary origin verifications, and maintaining transparency about hardware origins can build trust with customers and regulators.

"We have the Information Security Management System of ISO/IEC 27001:2013 and the Privacy Information Management System of ISO/IEC 27701:2019. Moreover, [we have] obtained TRUSTe privacy certification and ISO/SAE 21434:2021 certification for automotive industry cybersecurity."

Key leading vendor quote about meeting international security certifications

Holistic approach

To ensure its whole security solution—both software and hardware approaches—works and that other known vulnerabilities are not present, vendors should commission authorized pen tests. The results of these tests can help address identified gaps, which can satisfy EO 14028 and EU CRA recommendations and requirements.

"One of our modules has passed testing by TÜV SÜD based on EN 18031 standards and has successfully been certified for RED DA requirements. Other modules are being tested by other world-leading testing and certification companies."

Key leading vendor quote about testing

In adopting these comprehensive practices, IoT module vendors can take a proactive approach not only for regulatory compliance but also to ensure the security and reliability of their modules for the sake of their customers.

About IoT Analytics

IoT Analytics, founded and operating out of Germany, is a leading global provider of market insights and strategic business intelligence for the IoT, AI, the cloud, edge technology, and Industry 4.0.

Learn more about us
Visit our website: **www.iot-analytics.com**

About Quectel

Quectel's passion for a smarter world drives us to accelerate IoT innovation. A highly customer-centric organization, we are a global IoT solutions provider backed by outstanding support and services. Our growing global team of 5,600 professionals sets the pace for innovation in cellular, GNSS, satellite, Wi-Fi and Bluetooth modules, antennas and services. With regional offices and support across the globe, our international leadership is devoted to advancing IoT and helping build a smarter world.

For more information, please visit: **www.quectel.com**